Sign	Name	Value range		Practical range		Recommended
		Minimum	Maximum	Minimum	Maximum	
t	token length (bits)	2	none	6	12	8
b	block length (tokens)	2	none	$2^{(t/2)}$	$n2^{(t/2)}$	2^{t-1} (=128, if t=8)
a	number of authentication tokens	0	b-1	0	2	1
	position of authentication tokens	0	b-a-1	0	b-a-1	
c	number of copies	2	t	2	t	2
	pattern for token rearrangement					halves
	segment rotation pattern					all to the right
	block rotation direction	left	right	left	right	right

Figure 1. Some parameters and recommended values

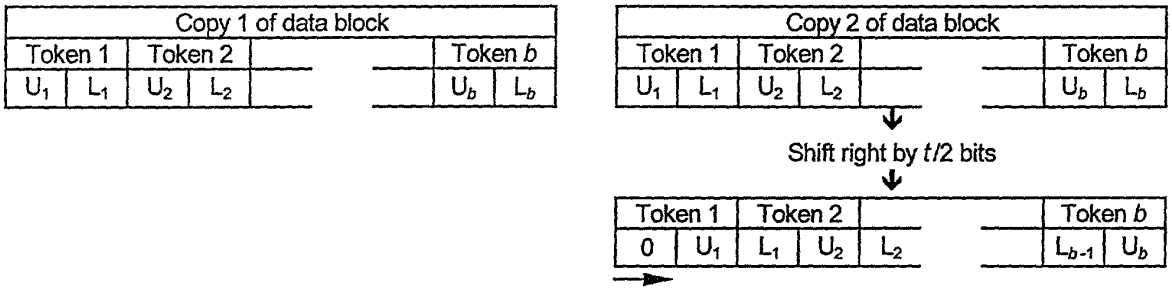

Figure 2. Creating a duplicate data block and shifting the upper half bytes into the lower ones in block 2

Value added	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Tokens in copy 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
Tokens in copy 2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

Figure 3. Effective values added to the lower half tokens

Upper half	Lower half
Random bits	$(v + l) \bmod (2^{t/2})$

Figure 4. Contents of a token after step 3

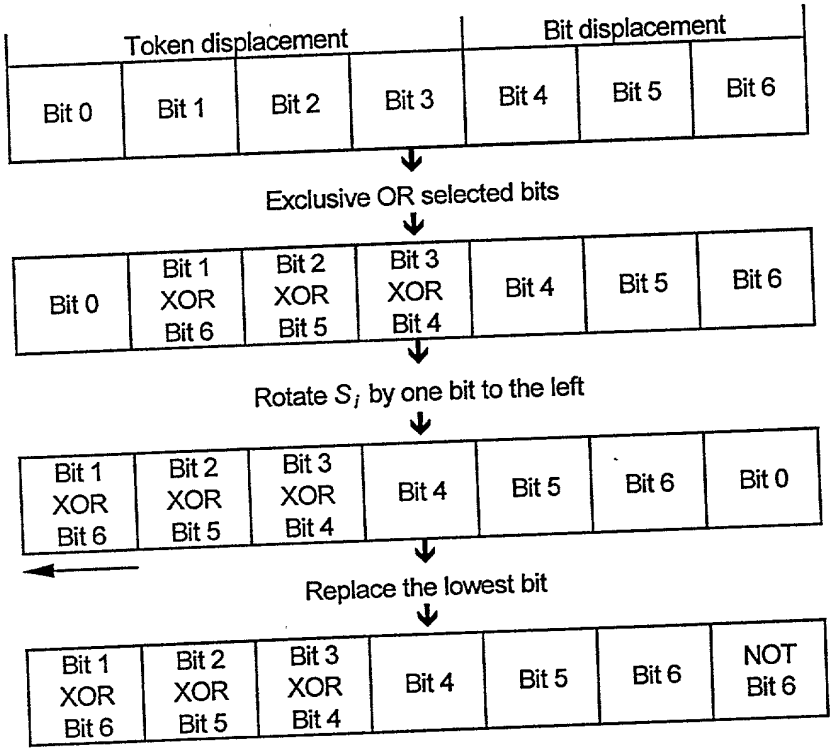

Figure 5. Changes to the value of S_i

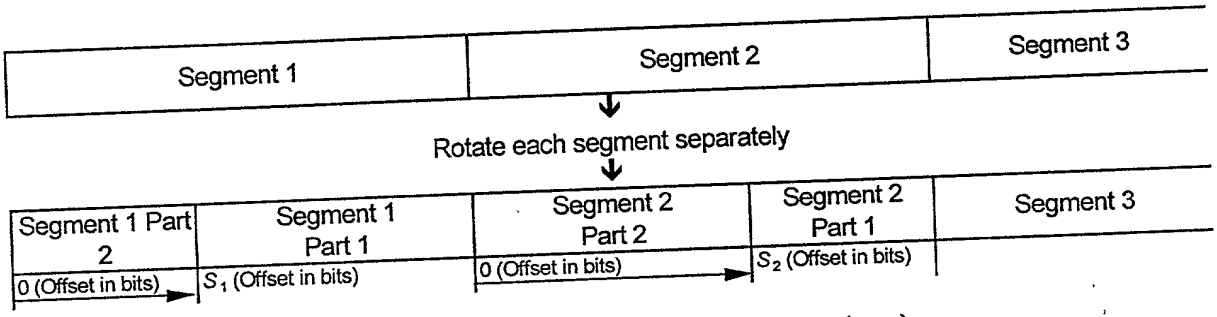

Figure 6. Rotations of the segments (right rotations shown)

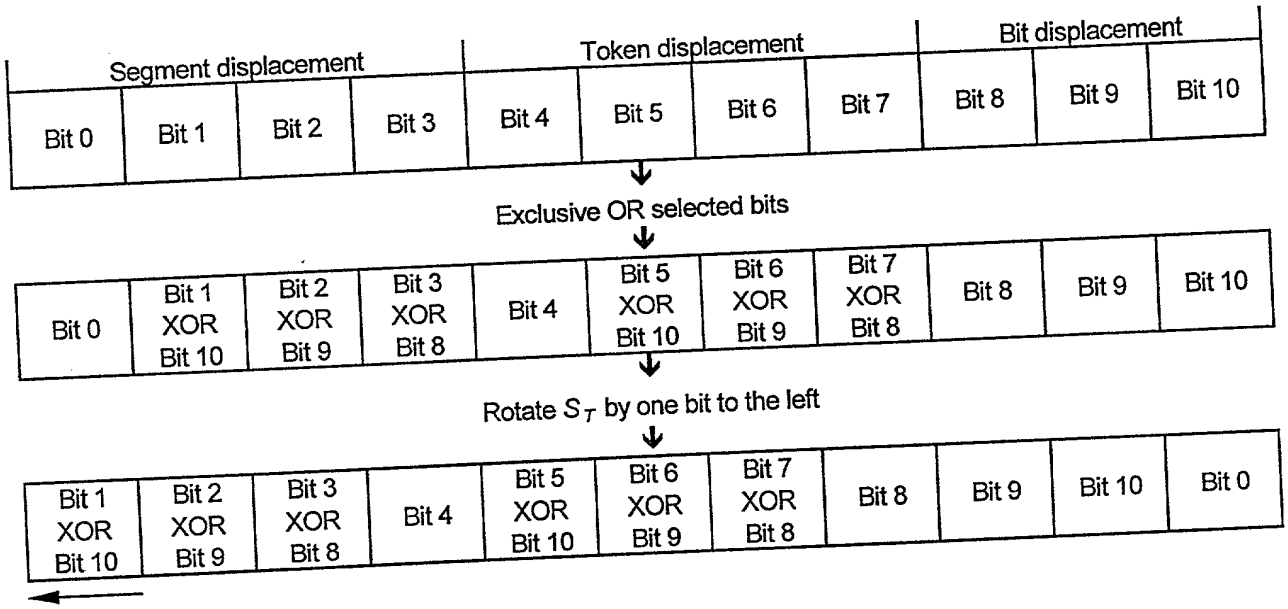

Figure 7. Changes to the value of S_T

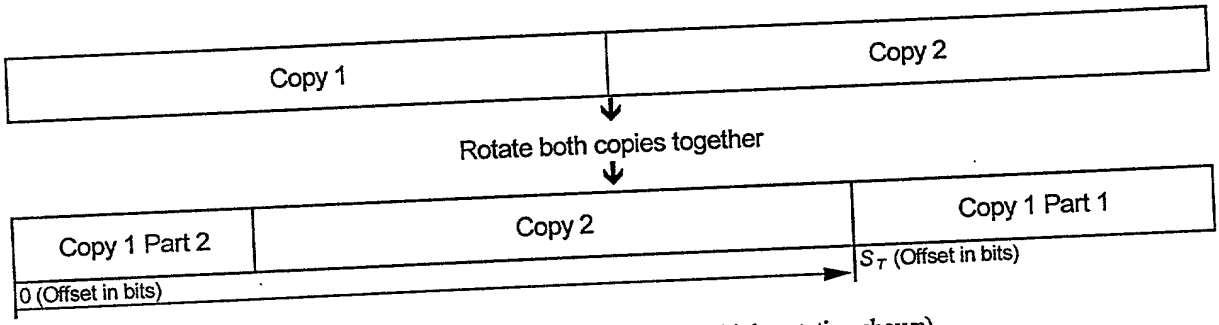

Figure 8. Rotation of the complete block (right rotation shown)

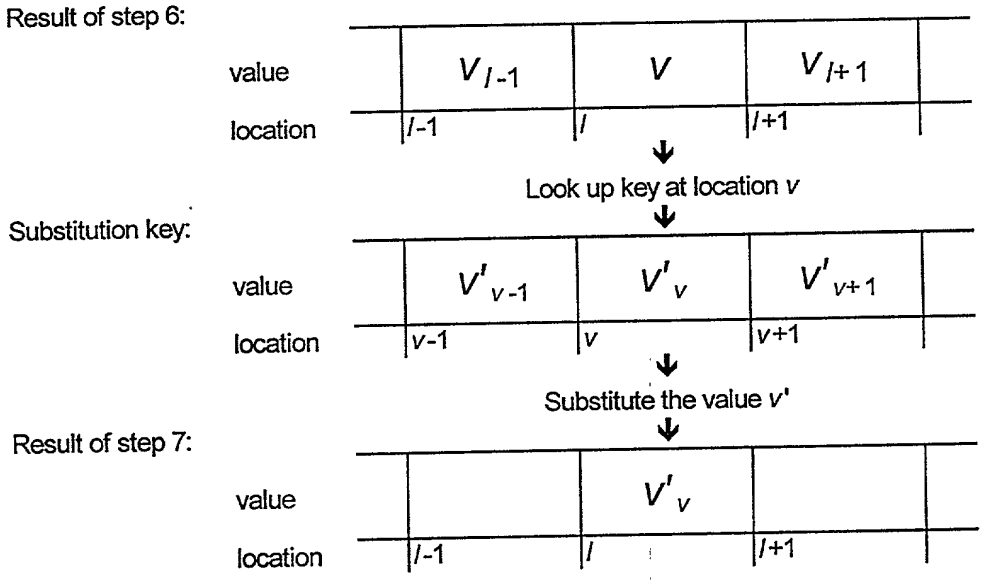

Figure 9. A token subtitution

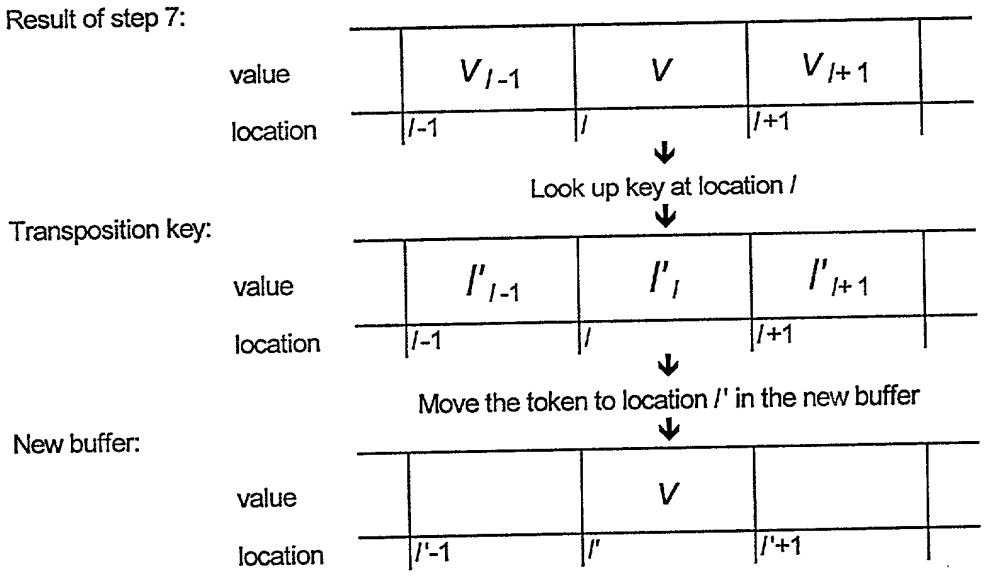

Figure 10. Moving a token during transposition

Transposition key:

value		l'_{l-1}	l'	l'_{l+1}	
location		$l-1$	l	$l+1$	

Reversal key:

value			l		
location		$l'-1$	l'	$l'+1$	

Figure 11. Relation between the transposition key and its reversal key

Substitution key:

value		V'_{v-1}	V'	V'_{v+1}	
location		$v-1$	v	$v+1$	

Reversal key:

value			V		
location		$v'-1$	v'	$v'+1$	

Figure 12. Relation between the substitution key and its reversal key